Sessional Assignment 2020

Subject: Advance Computer Networks (MS EE)

Marks:20

Submission date: 08th June 2020

Note: Attempt all Questions

Q1: Differentiate between a Hub, Switch and Router?

Q2: What does a backbone network means?

Q3: Explain the protocols used at different TCP/IP layers?

Q4: What is anonymous FTP?

Q5: What is subnet mask?

Q6: What is NAT?

Q7: Differentiate between TCP and UDP?

Q8: What is RIP and its key features?

Q9: Explain what is a firewall?

Q10: What is NOS?

Q11: What is Denial of Service (DoS)?

Q12: What is piggybacking?

Q13: What is DNS?

Q14: What is OSPF?

Q15: What is a ping?

Q16: In a network that contains two servers and twenty workstations, where is the best place to install an Anti-Virus program?

Q17: What is the difference between CSMA/CD and CSMA/CA?

Q18: What is RSA Algorithm?

Q19: What are the components of Protocol?

Q20: What is Tunnel mode?

Question: No: 01

Answer:

Hub vs Switch:

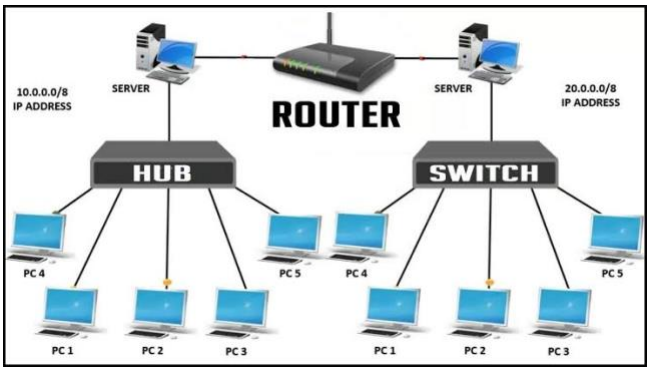
A hub works on the physical layer (layer 1) of OSI model while switch works on the data link layer. Switch is more efficient than the hub. A switch can join multiple computers within one LAN and a hub just connects mutiple ethernet device together as a single segement. Switch is smarter than hub to determine the target of the forwarding data. Since switch has higher performance, its cost will also become more expesive.

Switch vs Router:

In the OSI model router is working on a higher level of network layer than switch. Router is very different from the switch because it is for routing packet to other networks. It is also more intelligent and sophisticated to0 serve as an intermediate destination to connect multiple area networks together. A switch is only used for wired network, yet a router can also link with the wireless network. With much more functions, a

Hub vs Router:

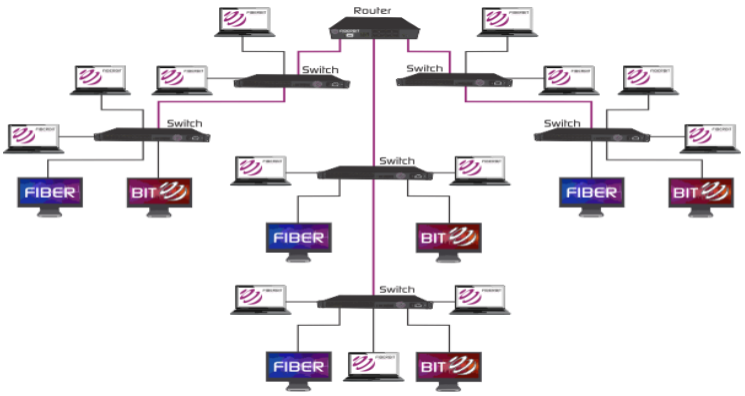
As mentioned above, a hub only contain the basic function of a switch. Hence differences between hub and router are even bigger. For instance, hub is a passive device without software while router is a networking device and data transmission form in a hub is in electrical signal or bits while in router it is in form of packet.



Question: No: 02

Answer:

The word backbone means the most important part of a system that provides the core support for the rest of the system. Like the backbone of the human body that holds and balances all body parts together the same holds true for networks. A backbone network is a network containing a high capacity connectivity infrastructure that forms the main link or backbone to the different parts of the network. The network consists of various LANs, WANs and sub network. The connectivity may cover a local area within a building or vicinity or may have a global outreach that spans vast geographical areas. The backbone has a capacity that far exceeds that of the individual networks connected to it. A backbone network normally consists of cabling, switches, bridges, router, and gateways in varying segments. Individual nodes do not connect directly to the backbone but do so through their LANs and ISPs or larger organizational infrastructures. Let’s examine the different networks that can be integrated with backbone technology.



Question: No: 03

Answer:

The TCP/IP protocol suite consists of many protocol that operate at one of 4layers.

The protocol suite is named after two of the most common protocol TCP and IP.

TCP/IP Layers	TCP/IP Prototocols				
Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Transport Layer	TCP		UDP		
Network Layer	IP		ARP	ICMP	IGMP
Network Interface Layer	Ethernet		Token Ring	Other Link-Layer Protocols	

TCP/IP was designed to be independent of networking hardware and should run across any connection media.

The earliest use and common use is over Ethernet networks. Ethernet is a 2 layer protocol /standard covering the physical and data link layer, shown in diagram above.

HTTP: this is the workhorse of the web.

SMTP, POP3, IMap4: These are email protocols.

TCP is a connection orientated protocol and is used to provide a reliable end to end connection.

UDP (used datagram protocol) is connection less protocol and does not guarantee delivery.

Application will choose which transmission protocol to use based on their function. HTTP, POP3, IMAP4, SMTP and many more used TCP.

UDP is used more in utility application like DNS, RIP (routing information protocol), and DHCP.

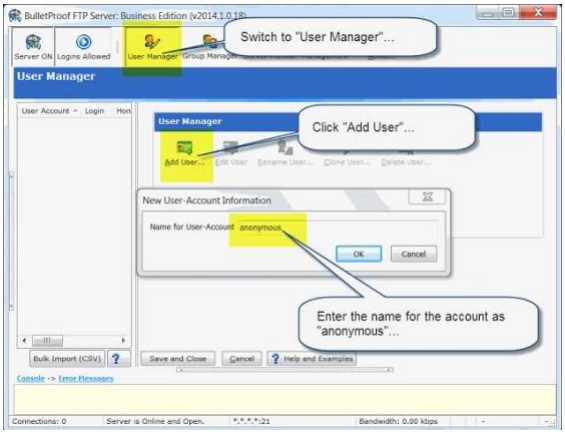
IP (internet protocol): this is the main networking protocol. There are two version of IP (IPv4 and IPv6).

The TCP/IP protocol suit is a collection of protocols that are used on the internet. It is named after two of the main protocols (TCP and IP) and uses a 4 layer networking model.

Question: No: 04

Answer:

Anonymous FTP (file transfer protocol) is a method for giving users access to file so that they do not need to identify themselves to the server. Using an FTP program or the FTP command interface, the user enters “anonymous” as a user ID. Usually, the pasword is defaulted or furnished by the FTP server. Anonymous FTP is a common way to get access to a server in order to view or download files that are publicly available.If someone tells you to use anonymous FTP and gives you the server name, just remember to use the word “anonymous” for your user ID. Usually you can enter anything as a password.



Question: No: 05

Answer:

Subnet mask and prefix length are two different ways of representing the same information which is to define the network portion of an IP address. A subnet mask is also a 32 bit number that tells the router which bits of the IP address are for the network portion and which bits are for the host portion. Subnet mask is a binary number but is also usually communicated in dotted decimal format or CIDR format.

Example subnet mask in dotted decimal: 255.255.255.0

In binary: 11111111 11111111 11111111 00000000

Value 1 in the subnet mask represents bit position of the network portion.

Value 0 in the subnet mask represent bit position of the host portion.

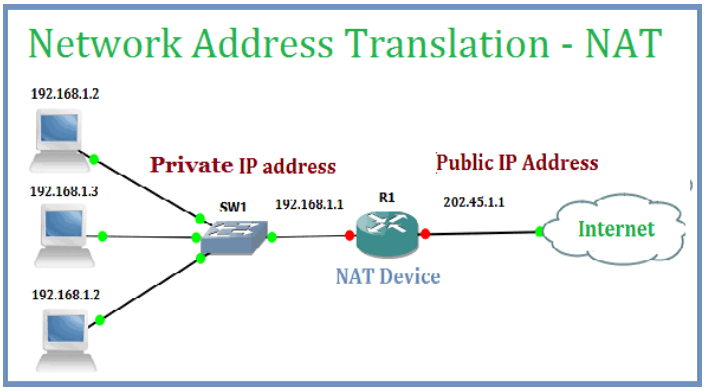
Question: No: 06

Answer:

Stand for “network address translation” NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connected the computers to the internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computer on the internet attempt to access computers within the local network, they only seethe IP address of the router. This adds an extra level of security since the router can be configured as a firewall, only allowing authorized systems to access the computer with in network.

Once a system from outside the network has been allowed to access a computer within the network, the IP address is then translated from the router address to the computers unique address. The address is found in a "NAT table" that defines the internet IP addresses of computers on the network. The NAT table also defines the global address seen by computers outside the network. Even though each computer within the local network has a specific IP address, external system can only see one IP address when connecting to any of the computer within the network.

To simplify, network address translation makes computers outside the local area network (LAN) see only one IP address, while computers within the network can see each systems unique address. While this aids in network security, it also limits the number of IP addresses needed by companies and organization. Using NAT, even large companies with thousands of computer can use a single IP address for connecting to the internet. Now that's efficient.



Question: No: 07

Answer:

Transmission control protocol (TCP):

1) TCP is a connection oriented protocol, which means the devices should open a connection before transmitting data and should close the connection gracefully after transmitting the data.
2) TCP assure reliable delivery of data to the destination.
3) TCP protocol provide extensive error checking mechanisms such as flow control and acknowledgment of data.
4) Sequencing of data is a feature of TCP.
5) Delivery of data is guaranteed if you are using TCP.
6) TCP is comparatively slow because of these extensive error checking mechanisms.
7) Multiplexing and demultiplexing is possible in transmission control protocol using TCP port numbers.
8) Retransmission of lost packets is possible in TCP.

User datagram protocol (UDP):

1) UDP is datagram oriented protocol with no overhead for opening a connection (using three-way handshake), maintaining a connection , and closing (terminating) a connection.
2) UDP is efficient for broadcast/multicast type of network transmission.
3) UDP has only the basic error checking mechanism using checksums.
4) There is no sequencing of data in UDP.

5) The delivery of data cannot be guaranteed in UDP.
6) UDP is faster, simpler and more efficient than TCP. However, UDP it is less robust then TCP.
7) Multiplexing and demultiplexing is possible in UDP using UDP port numbers.
8) There is no retransmission of lost packets in UDP.

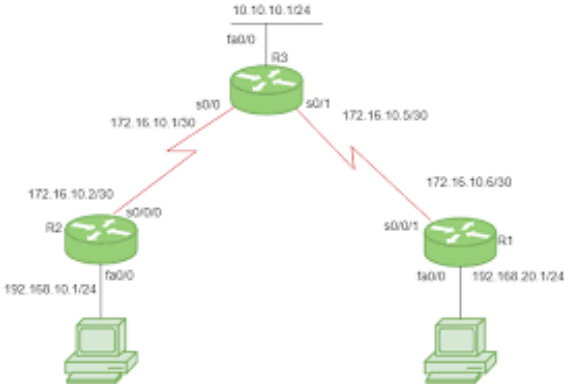
Question: No: 08

Answer:

Routing prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.

RIP v1	RIP v2	RIPng
Classful	classless	classless
Routing	protocol,	updates are sent
Protocol	supports classful	

And its key features is eagle RIP v8 has PDF 1.5 RIP, besides all features in PDF 1.4, for example, transparency,128-bit encryption and so on, the new RIP core support all PDF 1.5 features, for example, JPEG2000 filter, cross-reference stream, and so on.



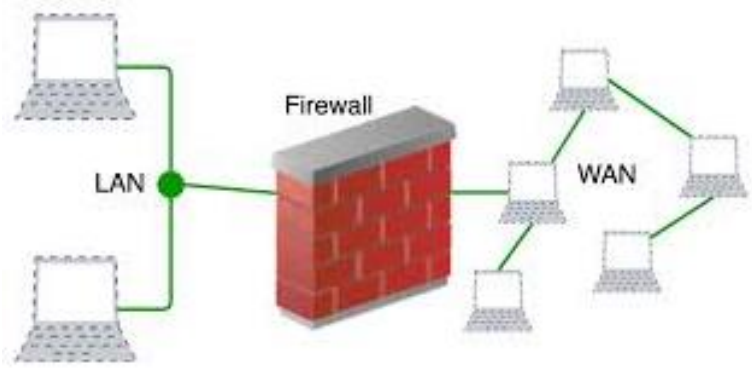
Question: No: 09

Answer:

A firewall is software used to maintain the security of a private network. Firewalls block unauthorized access to or from private network and are often employed to prevent unauthorized web users or illicit software from gaining access to private networks connected to the internet. A firewall may be implemented using hardware, software, or a combination of both.

Firewalls generally use two or more of the following methods:

- Packet filtering: firewalls filter packets that attempts to enter or leave a network and either accept or reject them depending on the predefine set of filter rules.
- Application gateway: the application gate way technique employs security methods applied to certain applications such as telnet and file transfer protocol severs.
- Circuit-level gateway: A circuit-level gateway applies these methods when a connection such as transmission control protocol is established and packets start to move.



Question: No: 10

Answer:

A network operating system (NOS) is a computer operating system that is designed primarily to support workstation, personal computer and in some instances, older terminals that are connected on a local area network (LAN). The software behind a NOS allows multiple devices within a network to communicate and share resources with each other.

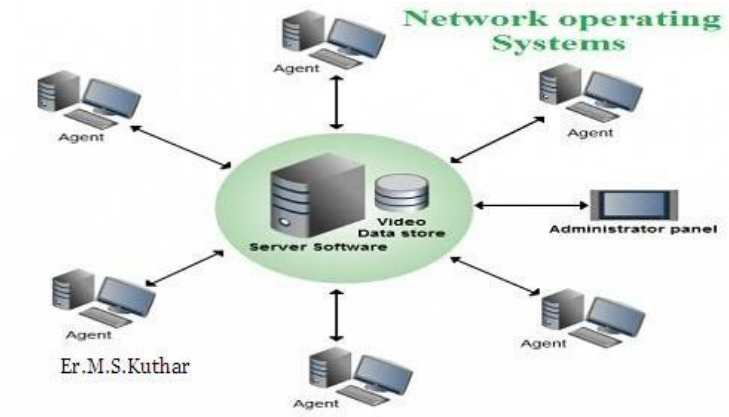
The composition of hardware that typically uses a NOS includes a number of personal computers, a printer, a server and file server with a local network that connects them together. The role of the NOS is to then provide basic network services and feature that support multiple input requests simultaneously in a multiuser environment.

Due to earlier versions of basic operating system not being designed for network use, network operating system emerged as a solution for single user computers.

Types of network operating systems:

There are two basic types of network operating systems.

The peer to peer NOS and the client/server NOS



Question: No: 11

Answer:

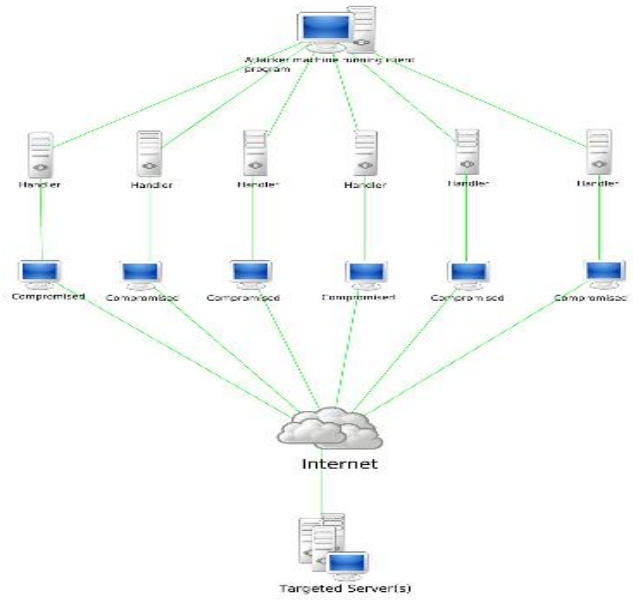
In computing a denial of service (DOS) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting service of a host connected to the internet. Denial of service is typically accomplished by flooding the targeted machine or resource

with superfluous requests in an attempt to users by temporarily or indefinitely disrupting services of a host connected to the internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or illegitimate requests from being fulfilled.

In a distributed denial of service attack the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simple by blocking a single source.

A DOS or DDOS attack is analogous to a group of people crowding the entry door of shop, making it hard for legitimate customers to enter, thus disrupting trade.

Criminal perpetrators of DOS attack often target sites or services hosted on high profile web servers such as bank or credit card payment gateway.



Question: No: 12

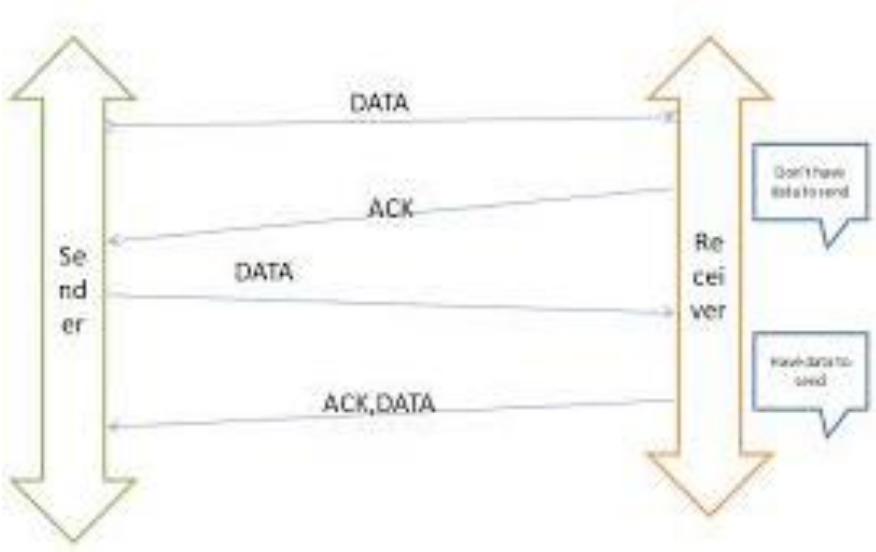
Answer:

Piggybacking means to ride over something. In a real example, if someone already traveling towards a destination, with his bike where you also need to reach, you just take the lift over the bike. If someone not traveling, then you use your own bike for the ride. A similar concept is very common in computer networks called piggybacking. In piggybacking, the sender send a data packet along with the acknowledgment, if any acknowledgment needs to send at the time of transmission of the data packet.

In reliable communication, each packet has an acknowledgment from the receiver. SCTP protocol is one example of a reliable transport layer protocol in the OSI model.

Piggybacking is an optimization method for the utilization of underling network capacity. A user message is piggybacked over an acknowledge message.

For example, in SCTP a single message may have two chunks one is for DATA and the other is ACK. After piggybacking, there is a single message over the wire in place of two.



Question: No: 13

Answer:

The domain name system (DNS) is the phonebook of the internet. Humans access information online through domain names, like nytimes.com or espn.com web browsers interact through internet protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load internet resources.

Each device connected to the internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4) or more complex newer alphanumeric IP addresses such as 2400:cb00:2048::c629:d7a2 (in IPv6)

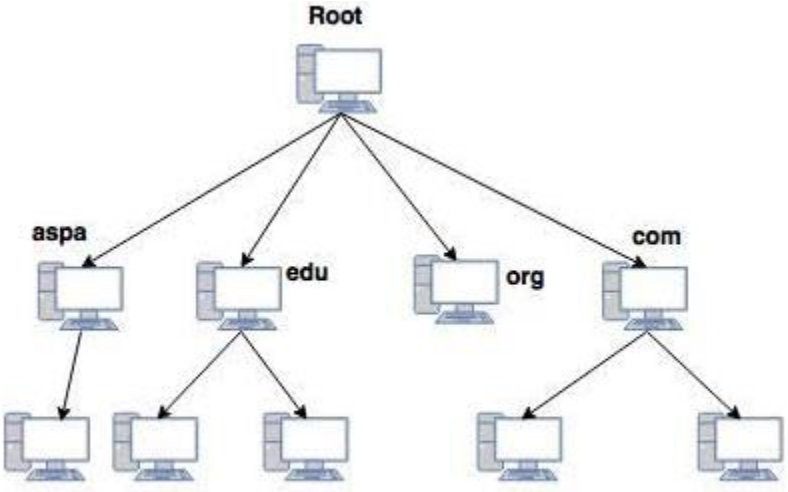


Fig: Hierarchy of DNS

Question: No: 14

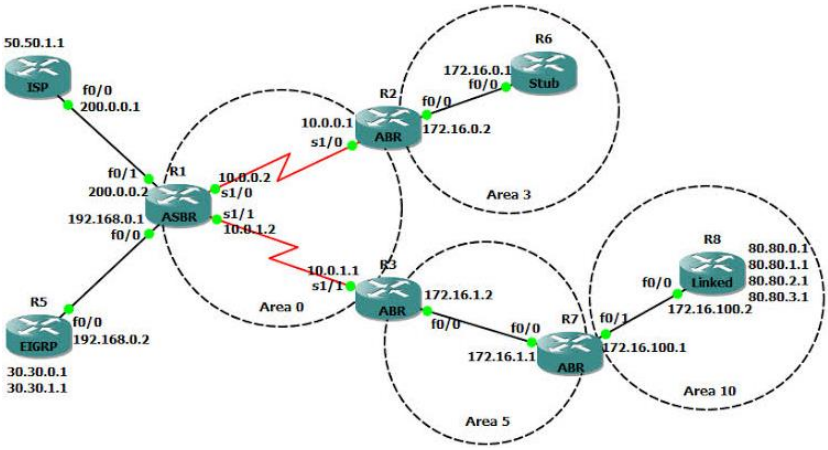
Answer:

Open short path first (OSPF) is a link state routing protocol that is used to find the best path between the source and the source and the destination router using its own shortest path first. OSPF is developed by internet engineering task force (IETF) as one of the interior gateway protocol (IGP),i.e., the protocol which aims at moving the packets within a large autonomous system or routing domain. It is a network layer protocol which work on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router (DR)/backup designated router (BDR)

OSPF terms:

1. Router Id: It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.
2. Router priority: it is a8 bit value assigned to router operating OSPF, used to elect DR and BDR in a broadcast network.
3. Designated router (DR): It is elected to minimize the number of adjacency formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other router shares their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.
4. Backup designated router (BDR): BDR is backup to DR in a broadcast network. When DR goes to down, BDR becomes DR and perform its function.

DR and BDR election: DR and BDR election takes place in broadcast network or multi-access network. Here are the criteria for the election.



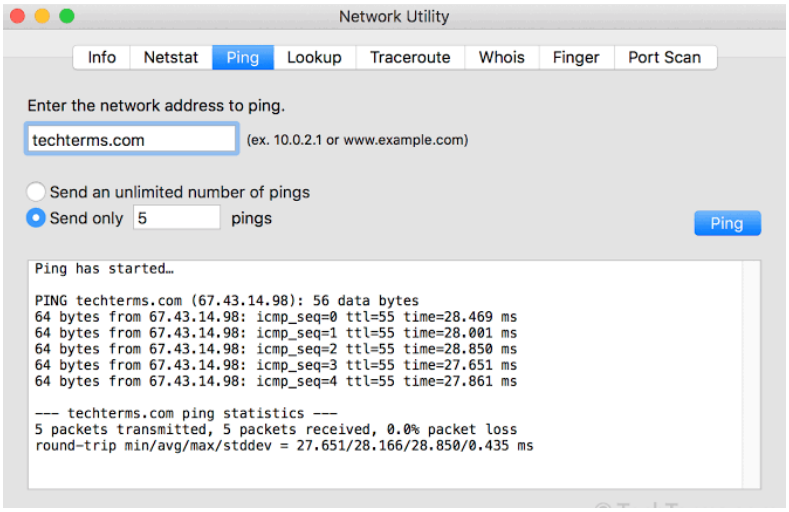
Question: No: 15

Answer:

Ping is a network utility program or a tool to test if a particular host is reachable. It is a diagnostic that checks if your computer is connected to a server. Ping a term taken from the echo location of a submarine, sends data packet to a server and if it receives a data packet back, then you have a connection. The term ping can refer to the time it takes for a data packet to travel round trip. It means get the attention of or check the presence of. In computer network, a ping test is a way of sending message from a computer to another. Aside from checking if the computer is connected to a network, ping also gives indicators of the reliability and general speed of the connection.

Ping Test:

A ping test is a method of checking if the computer is connected to a network. It also determines the latency or delay between two computers.it is used to ensure that a host computer which your computer tries to access is operating. A ping test is run for troubleshooting to know connectivity as well as response time.



Question: No: 16

Answer:

You need at least three levels of security.

1. A good firewall. This can stop intrusions, malware, unauthorized access, etc. before they reach the workstations.
2. Antivirus software on the servers and at the end point workstations. This software should be centrally managed to keep end users updated constantly and to minimize user meddling with the settings. Good antivirus will also protect email clients.
3. Educated and aware users who: do not casually install downloaded programs; do not click on unknown links; do not fall for phishing email etc. establish a strong password policy for all users. You should consider not giving your users administrative rights on their accounts. They will complain that they cannot install what they need and your workload will increase but I guarantee you, your entire environment will be more reliable and secure.

Remember: your computing environment is only as secure as your weakest link and non-compliant user.

Question: No: 17

Answer:

The difference between CSMA/CD and CSMA/CA

CSMA/CD	CSMA/CA
CSMA/CD is effective after a collision.	Whereas CSMA/CA is effective before a collision.
CSMA/CD is used in wired networks.	Whereas CSMA/CA is commonly used in wireless networks.
It only reduces the recovery time.	Whereas CSMA/CA minimizes the possibility of collision.
CSMA/CD resend the data frame whenever a conflict occurs.	Whereas CSMA/CA will first transmit the intent to send for data transmission.
CSMA/CD is used in 802.3 standard.	While CSMA/CA is used in 802.11standard.
It is more efficient than simple CSMA(carrier sense multiple access)	While it is similar to simple CSMA(carrier sense multiple access)

Question: No: 18

Answer:

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name RSA algorithm.

Algorithm:

The RSA algorithm holds the following features:

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

You will to go through the following steps to work on RSA algorithm.

Step 1: Generate the RSA modulus:

The initial procedure begins with selection of two prime numbers namely p and q and then calculating their product N as shown.

$N=p\times q$

Here let N be the specified large number.

Step 2: Derived number (e):

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1.

Step 3: Public key

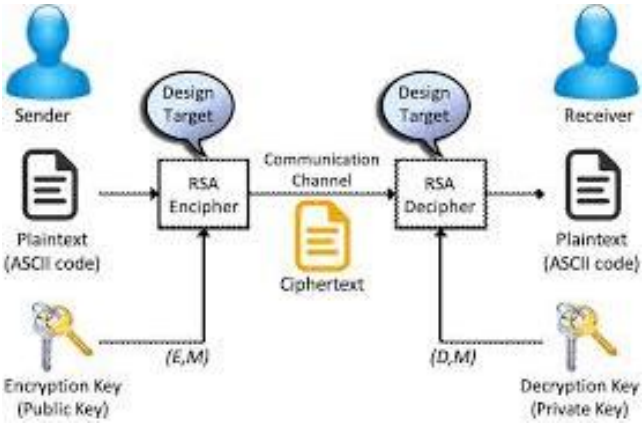
The specified pair of numbers n and e forms the RSA public key and it is made public.

Step 4: private key

Private Key d is calculated from the numbers p, q and e. the mathematical relationship between the numbers is as follows.

ed= 1 mod (p-1) (q-1)

The above formula is the basic formula for extended Euclidean algorithm. Which takes p and q as input parameters.

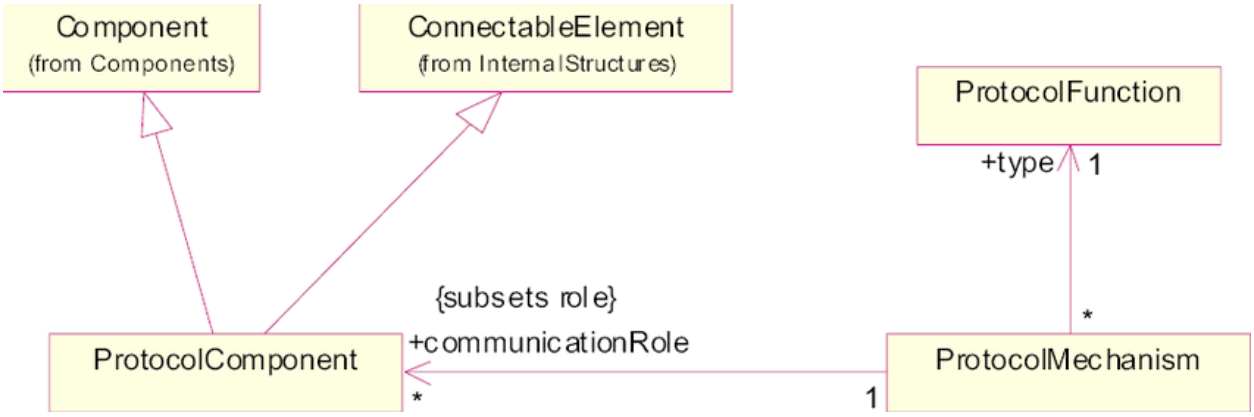


Question: No: 19

Answer:

The components of protocol is:

Title page	Background information	Objectives and purpose	Study design and end points	Study enrollment and withdrawal
Study procedures and schedule	Efficacy assessment	Safety assessment	Clinical monitoring	Statistics analysis
Source documents and access	Quality control and assurance	Ethics/protection of human subjects	Data handling and record keeping	Publication policy
Study administration	Reference	Supplements/appendices		



Question: No: 20

Answer:

Tunneling is a protocol that allows for the secure movement of data from one network to another. Tunneling involves allowing private network communications to be sent across a public network, such as the internet, through a process called encapsulation. The encapsulation process allows for data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through unnoticed.

Tunneling is also known as port forwarding.

In tunneling, the data are broken into smaller pieces called packets as they move along the tunnel for transport. As the packets move through the tunnel, they are encrypted and another process called encapsulation occurs. The private network data and the protocol information that goes with it are encapsulated in public network transmission units for sending. The units look like public data, allowing them to be transmitted across the internet. Encapsulation allows the packets to arrive at their proper destination. At the final destination, de-capsulation and decryption occur